Мошенничество в сфере IT-технологий

Тенденция развития информационных технологий в последнее время влечет повсеместное их вовлечение во многие сферы общественных отношений, что сказывается не только на удобстве для добросовестных пользователей, но и служит почвой для противоправной деятельности, выражающейся в незаконном обогащении, дискредитации граждан и государственных органов, распространении запрещенной информации, в том числе, идей экстремизма и терроризма.

Как в целом по стране, так и на территории Омской области отмечается ежегодный рост таких преступлений, к которым также относятся хищения денежных средств с банковских счетов физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.

Рассмотрим пять основных способов, которыми пользуются мошенники при похищении денег.

Первой преступной схемой является информирование граждан по телефону о несанкционированных попытках оформления на граждан кредитов, о фиксации системой безопасности незаконного доступа к их счётам, а также конфиденциальным данным. Мошенники убеждают людей оформить кредит, чтобы вернуть деньги банку, якобы незаконно оформленные преступниками. Кроме того, злоумышленники могут попросить провести операции через банкомат и «Мобильный банк».

Отметим, мошенники могут звонить с подменных телефонных номеров, которые будут определяться как телефоны дежурной части полиции. Они рассказывают о расследовании уголовного дела по факту якобы мошенничества и о том, что сотрудниками безопасности банка зафиксированы несанкционированные попытки доступа третьих лиц к его счету. После этого предупреждают о необходимости оказания содействия сотрудникам банка, которые свяжутся с ним позже.

Звонок от представителя правоохранительных органов убеждает жертву в серьёзности происходящего, поэтому дальнейший звонок от «сотрудников службы безопасности банка» не вызывает подозрений.

Вторая схема - мошенничество при покупке и продаже товаров в интернете. Преступники, предлагая товар, просят за него предоплату или полную стоимость, а потом пропадают. Либо наоборот - связываются с продавцом под видом покупателя и предлагают оформить «безопасную сделку». Для ее оформления сбрасывают ссылку на фишинговый сайт, где после оформления формы со счетов списываются деньги.

Третьей схемой является мошенничество в социальных сетях. Например, преступники предлагают принять участие в розыгрыше или акции, и опять же через фишинговые сайты похищают деньги. Другой вариант - взлом аккаунта в соц. сетях и рассылка просьб друзьям и родственникам потерпевшего об одолжении денег.

Четвёртая схема - поддельные сайты трейдерских бирж. Преступники делают предложения о быстром заработке путём спекуляции на курсе валют и акций. В итоге у жертвы похищаются все средства, имеющиеся на банковском счету.

Пятой и одной из самых распространённых схем мошенников является звонок жителям региона с сообщением о неприятностях, в которые якобы попали их родственники. Например, говорят о том, что дети или внуки стали виновниками ДТП и чтобы избежать последствий в виде проблем с законом, нужно заплатить деньги. Чуть позже приезжает якобы курьер и забирает необходимую сумму.

Напомним, в основном к совершению подобных преступлений причастны жители других регионов России, которые выступают в мошеннических схемах в качестве «курьеров»: забирают деньги у потерпевших и переводят их на счета соучастников.

Напоследок в очередной раз предостеречь граждан от возможного хищения денег. Если вам поступил подозрительный звонок – лучше положить трубку и перезвонить на горячую линию банка либо в дежурную часть полиции, номера которых имеются сейчас в открытом доступе. В случае с телефонным сообщением о том, что родственник попал в ДТП, лучше сначала связаться с ним для уточнения информации.

Чтобы ни происходило – не отключать логику и сохранять спокойствие. Предосторожность и предусмотрительность – лучший друг вашей безопасности.